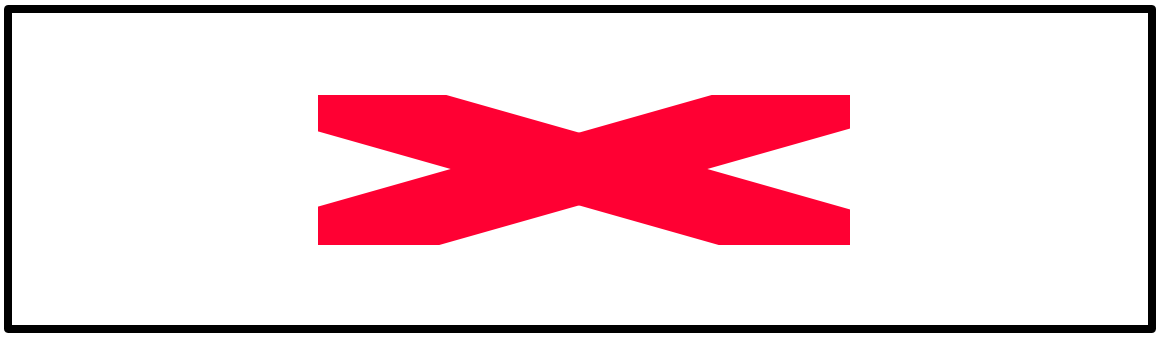

Testimony and Statement for the Record of

Marc Rotenberg
Electronic Privacy Information Center, Executive Director
Georgetown University Law Center, Adjunct Professor

Hearing on
Information Privacy

Before the

Committee on Commerce, Science and Transportation
United States Senate

July 11, 2001
253 Russell Senate Office Building

My name is Marc Rotenberg. I am Executive Director of the Electronic Privacy Information Center (EPIC) in Washington. I have taught the Law of Information Privacy at Georgetown University Law Center since 1990. I am the editor of two books on privacy and have participated in many of the public campaigns over the past decade to safeguard privacy rights in the United States.

I'd like to thank the Committee for holding this hearing today and also for the hearings that were held during the past Congress to address public concerns about privacy. This is an enormously important issue of interest to a great many Americans. Simply stated, there is a widespread concern that in order to enjoy the benefits of information technology we will be forced to sacrifice personal privacy. The central challenge is how best promote the benefits of new technology and to preserve right of privacy and personal autonomy.

I believe that there are two questions before the Committee today. The first is whether legislation is necessary to protect privacy on the Internet. The second, if you agree that legislation is appropriate, is what are the key elements of a good privacy measure. I will focus my remarks on these two issues.

1. The Need for Privacy Legislation

a. Legal tradition

Legal tradition in the United States clearly shows that laws will be established to safeguard the right of privacy when new electronic services are provided. This was true in 1934 when the Congress adopted provision 605 of the Communications Act to ensure the privacy of communications sent by telephone and in 1999 when Congress passed the Wireless Communications and Public Safety Act to safeguard the privacy of location data in advanced network services.

With virtually every new technology that involved the collection of personal consumer information – from Cable television and video rentals to electronic mail and automated medical information – Congress has passed laws to safeguard privacy. It has established clear responsibilities for companies that collect personal information and has created rights backed up with legal sanctions for individuals who disclose information in the course of a commercial transaction.

These laws have promoted best business practices, promoted public confidence, and limited the misuse of personal information in the new electronic environments. In other words, these laws have encouraged public adoption of new services to the benefit of both consumers and businesses.

Some have said that there should not be different rules for the online world and the offline world, but there are two answers to this point. First, online commerce simply is different. Cookies, web bugs, online profiling and Spyware are all uniquely associated with the architecture of the interactive digital environment. Publishers in the print and broadcast media simply do not have the ability to collect personally identifiable information without the actual consent or participation of their customers. A newspaper advertiser does not know who was reading an ad.

But today with the Internet, advertisers do have the ability to track individuals. Techniques are available to profile individual preferences, oftentimes without the knowledge or consent of the profiled person. It is because of the very specific capability of the online environment to collect and record personal information that legislation is appropriate. And it is consistent with the tradition of US privacy law that such legislation be adopted.

b. Technology and Legislation Work Together

Key to the adoption of privacy legislation is that lawmaking and technological innovation can work together. Groups, such as EPIC, that favor privacy legislation have also worked to encourage the development of technical standards that allow Internet users to safeguard their data and protect their identity. One of the most popular features on our web site is the Practical Privacy Tools page which allows Internet users to surf anonymously, delete cookies, encrypt private messages, erase files, and filter ads.

We recognize that there are a range of technical and legal approaches that will help safeguard privacy. But we also believe that in the absence of a statutory framework, a type of privacy survivalism could easily result. Without consumer trust in new services, each person will be forced to adopt elaborate defensive measures to protect privacy in the most routine commercial transaction. Such an outcome could not be beneficial for the long-term growth of electronic commerce.

c. Public Opinion

There are very few issues today in which Americans have expressed a clearer opinion than on the issue of privacy. In poll after poll, the public has made clear that it is concerned about the loss of personal privacy and that it believes it is appropriate and necessary for the government to act. Large majorities are found in both political parties.

According to the Pew Internet and American Life Project, 86% of Internet users favor opt-in privacy policies. According to Businessweek, three times as many Americans believe the government should pass laws now to safeguard online privacy as those who believe self-regulation is sufficient. According to Forrester Research, 90% of Americans want the ability to control the collection and use of their data. The Pew survey also found that more than 90% of Internet users thought companies should be punished when they violate their own privacy policies.

In a recent Gallup Poll, 66% of email users said that the federal government should pass laws to protect citizens' privacy online. Most remarkable is that the Gallup organization found that support for legislation increased as the level of experience increased. Frequent Internet users – those who spend 15 hours or more online each week -- are more likely to favor the passage of new laws (75%) than are infrequent users (63%). This finding is contrary to some of the earlier industry-funded polls that attempted to suggest support for legislation would diminish as use of the Internet increased.

The message here is clear: experienced Internet users understand the limitations of technical solutions and industry self-regulation. They want legal control over their personal information.

d. Experience with Self-Regulation

The argument for legislation is also made clear by the failure of self-regulation to safeguard online privacy and promote public confidence in network services. Public concern about the loss of privacy has grown almost in direct proportion to the self-regulatory programs. In many respects, this is not surprising. These programs encourage the posting of privacy notices, which have come to be called privacy warning labels that provide little actual assurance of privacy protection. If you go to a website and read a privacy policy, you will see quickly that these policies simply state the many purposes to which the information collected will be used. Few privacy policies make any meaningful attempt to limit the use or disclosure of data obtained.

Technical problems are also arising with self-regulatory initiatives. How do you provide a privacy notice to a person who tries to access a web site from a cell phone, a commercial application that may become increasingly popular in the years ahead? One solution now under

consideration is to create special symbols that could be viewed on the cell phone display. Another privacy scheme sets out a confusing array of privacy choices that will likely exclude many people from commercial web sites where privacy rules could otherwise provide uniform protection.

Problems with self-regulation can also be found in certain market segments where industry has been left free to design its own privacy policies rather than to rely on better established legal frameworks. For example, the Network Advertising Initiative proposal sanctioned by the FTC allows Internet advertisers to continue to profile Internet users, based on only the availability of an opt-out opportunity. This is contrary to the general approach in other areas which establish legal obligations for those who create profiles on known individuals. Even more surprising is that to exercise a right to opt-out of routine tracking, Internet users must maintain on their computers a cookie from the company that would otherwise track them!

e. Government Searches

Many who oppose legislation for online privacy say they want to keep government off the Internet. But one practical consequence of failing to pass privacy legislation is that without legislation there is no protection for personal information held by third parties from government searches. Government agents are free to go to Microsoft, Yahoo, Amazon, or any company in possession of personal data without a warrant and obtain the data on these companies' customers whether or not it is directly relevant to a particular investigation. This is contrary to the approach that has been established for other new electronic services as well as the treatment of sensitive information in the offline world. It also demonstrates the failure of self-regulation: there is no procedure and no method of accountability when data is disclosed to third parties through legal compulsion.

f. The International Dimension

The need for privacy legislation is demonstrated also by the demands of global commerce which now allows consumers around the world to buy and sell products online. This is a very promising development but also raises substantial concerns about the protection of the personal information that flows across the network. Many governments have taken steps to develop privacy laws to safeguard consumer interests.

Although the US has not yet adopted legislation that might be considered adequate for purposes of the European Union Data Directive, the Safe Harbor Arrangement does offer a possible intermediate step that will provide some assurance of privacy protection for European consumers doing business with US firms. Moreover, US firms have realized that in adopting these standards for their relations with customers in Europe, it is now sensible to provide similar protections for customers in the United States.

Privacy legislation will help carry forward this process by encouraging firms to adopt standards for privacy protection that will be recognized in countries around the world. Establishing these privacy rules for the online marketplace will be critical for the continued growth of global commerce.

g. Emerging Challenges

Much of the privacy work of this Committee has focused on issues associated with the Internet. But there are new challenges ahead. A report from the Center for Digital Democracy makes clear that the televisions in homes that allow us to look out on the world will increasingly be looking back at us. Cameras in public places raise new challenges for local communities. Even the tracking of rental cars by GPS has provoked public concern.

I do not think Congress today can anticipate all of the new privacy challenges that will arise. But the passage of legislation to protect online privacy will carry forward an important tradition, strengthen public confidence, and provide the basis for future legislative efforts.

2. The Need for Good Internet Privacy Legislation

If the case is made for legislation to safeguard the rights of Internet users, then the next question is how best to draft the bill. Previous legislation enacted by Congress provides a blueprint for legislation in this area. These laws reflect a reasoned consideration of the key elements for privacy protection in a wide range of areas. They have also helped enforce best practices within industry segments, promote public confidence in new services, and minimize that risk that information will be used improperly.

a. Openness and accountability

The first requirement of a good privacy law is that organizations are open about their data collection practices and accountable to those whose information they gather. This is not simple a matter of posting a notice or a privacy policy on a web site.

The most effective way to ensure openness and accountability is to give the individual the right to inspect the data collected, ensure its accuracy and understand it use. This principle goes back to the Privacy Act of 1974 which grants every citizen the right to access and correct records maintained by federal agencies, 5 USC § 552a(d)(1-4), and to the Fair Credit Reporting Act of 1970 which gives consumers the right to access their credit reports maintained by credit reporting agencies. 15 USC § 1681g(a).

This approach has been carried forward in privacy legislation developed for new electronic services. The privacy provisions in the Cable Act of 1984, for example, establish the right for cable subscribers to "access all personally identifiable information regarding the subscriber collected and maintained by a cable operator." 47 USC § 551(d). The Children's Online Privacy Protection of 1999 allows parents to obtain records of information collected on their children and request that certain information be removed. 15 USC § 6502(b)(1)(B)(i),(ii).

The right to access information about oneself held by others in the context of a commercial relationship is one of the key elements of effective consumer privacy legislation.

b. Meaningful consent

Privacy law makes clear that consent must be meaningful and that this often requires prior express consent. For example, the Video Privacy Protection Act states that disclosure of personally identifiable information, such as the title or description of tapes rented, requires "informed, written consent of the consumer given at the time the time the disclosure is sought." 18 USC § 2710(b)(2)(B). The privacy provision in the Cable Act requires "prior written or electronic consent" before a cable operator may collect any personally identifiable information that is not necessary to provide the cable service or detect unauthorized interception of cable communications. 47 USC § 551.

One of the reasons that privacy advocates and experts favor the opt-in approach is that it follows the common sense understanding of consent. If you look up the dictionary definition for consent, you will likely see "permission," "approval," or "assent." All of these terms imply an overt act, not a failure to act. This is the approach typically followed in privacy statutes.

c. Private Right of Action

Privacy laws have also typically included a private right of action that has empowered individuals and made it possible to hold accountable those who misuse the personal information in

their possession. In crafting the liability provisions in privacy statutes, Congress has wisely incorporated a liquidated damages provision that provides a specific dollar figure for violations of the law. This is necessary because it is often difficult to assign a specific economic value to privacy harm.

The Cable Act, for example, allows for a civil action and the recovery of actual damages not less than liquidated damages of $100 per for violation or $1,000, whichever is higher. 47 USC § 551(f). The Video Privacy Protection Act specifies liquidated damages of $2,500. 18 USC § 2710(c)(2). The Telephone Consumer Protection Act allows individuals who receive unsolicited telemarketing calls to recover actual monetary loss for such violation or up to $500 in damages. 47 USC § 227(c)(5).

These awards are hardly exorbitant. But they do help ensure that the rights established by Congress will be backed up with remedies. In the absence of a private right of action, there is a very real risk that there will be little incentive for companies to comply with privacy standards.

d. Federal Baseline

Privacy laws enacted by Congress have typically not preempted state privacy laws. This is partly out of respect for our federal form of government that grants states authority to safeguard the rights of their citizens, and also out of recognition that states frequently innovate in areas of emerging privacy protection. The bill to address genetic privacy, for example, which has now received bipartisan support, came about in part through a process of trial and error in state legislatures. Similar experimentation in the best ways to address video surveillance is currently underway.

In the Cable Act, states and franchising authorities may take further steps to enact and enforce laws for the "protection of subscriber privacy." 47 USC § 551(g). The Video Privacy Protection Act will "preempt only the provisions of State or local law that requires disclosure" otherwise prohibited by the section. 18 USC § 2710(f). Even the Telephone Consumer Protection Act left the state Attorneys General free to bring actions under the Federal statute and made clear that nothing in that law would "prohibit an authorized state official from proceeding in State court on the basis of alleged violation of any general civil or criminal statute of such State." 47 USC § 227(f)(6).

e. Cable Act as Model

Mr. Chairman, almost twenty years ago you introduced legislation to safeguard the privacy rights of users of new interactive cable services. Similar legislation was introduced at that time by Senator Barry Goldwater and by Senator Howard Baker. There was no question at that time that in the interactive environment associated with cable television services in the early 1980s significant privacy issues would arise. Customers would bank online, cast votes online, and express their political opinions. Congress wisely established privacy rules to safeguard the collection and use of personal information in that emerging communications environment. The privacy provisions in the Cable Act, although filling only a few pages, provide just about the most extensive protection of privacy to be found in US law. 47 USC § 551. Under that law, every consumer in the United States who subscribes to a cable television service receives certain basic privacy rights.

Cable providers must provide written notice to subscribers of their privacy rights at the time they first subscribe to the cable service and, thereafter, at least once a year. These notices must specify the kind of information that may be collected, how it will be used, to whom and how often it may be disclosed, how long it will be stored, how a subscriber may access this information and the liability imposed by the Act on providers.

Subject to limited exceptions, the Act requires cable service providers to obtain the prior written or electronic consent of the cable subscriber before collecting or disclosing personally

identifiable information. The Act grants cable subscribers the right to access the data collected about them and to correct any errors. It also provides for the destruction of personally identifiable information if that information is no longer necessary. There is a clear Fourth Amendment standard that limits the circumstances under which government may gain access to our private viewing records. Finally, the law sets out a private right of action including actual and punitive damages, attorney's fees and litigation costs for violations of any of its provisions. State and local cable privacy laws are not preempted by the Act.

The privacy provisions in the Cable Act of 1984 make clear that Congress can pass sensible, workable and effective legislation for new interactive environments. It has done so on a bipartisan basis and those provisions have stood the test of time.

f. Consequences of Weak Legislation

It is conceivable that Congress would adopt a weak "notice and choice" privacy law that provides few substantive rights, preempts state law, and lacks a method of meaningful enforcement. Such a measure would likely produce the backlash that has resulted from the weak privacy provisions in the Financial Services Modernization Act. The warning notices mandated by that law have simply raised public awareness of the widespread sharing of personal information and the difficulty in protecting privacy under the opt-out approach. This approach fails to establish actual safeguards for personal data when it is collected.

The better approach is the one favored by forward-looking businesses and the one traditionally followed in privacy law: those who wish to make use of personal information have the affirmative responsibility to obtain meaningful consent, rights to access personal information held by others should be established, and methods for meaningful oversight should be established.

CONCLUSION

Mr. Chairman, Members of the Committee, the time has come to make clear that the right of privacy does not end where the Internet begins. There is now the chance to establish law that will allow users to enjoy the benefits of innovation and to preserve cherished values. We have the opportunity to carry forward an American tradition that has marched side by side with the advancement of new technology. But we may not have this opportunity for long. In the absence of clear legal standards, we could easily drift into a world of privacy notices and warning labels, where every keystroke on your personal computer is quietly recorded in the database of another computer, then to be merged with data beyond your knowledge or control. In the absence of good privacy legislation, that future seems likely.

Thank you for the opportunity to appear before the Committee. I will be pleased to answer your questions.

REFERENCES

Phil Agre and Marc Rotenberg, eds., *Technology and Privacy: The New Landscape* (MIT Press 1997).

Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press 1992).

EPIC Practical Privacy Tools
[http://www.epic.org/privacy/tools.html]

EPIC and Junkbusters, "Pretty Poor Privacy: An Assessment of P3P and Internet Privacy" [http://www.epic.org/Reports/prettypoorprivacy.html]

David H. Flaherty, *Protecting Privacy in Two-Way Electronic Services* (Knowledge Industry Publications 1985).

Gallup Organization, "Majority of E-mail Users Express Concern about Internet Privacy," June 2001 [http://www.gallup.com/poll/releases/pr010628.asp]

Privacy Coalition [http://www.privacypledge.org]

Privacy Site [http://www.privacy.org]

Marc Rotenberg, *The Privacy Law Sourcebook 2000: United States Law, International Law, and Recent Developments* (EPIC 2000).

Marc Rotenberg, "Can We Keep a Secret?" *American Lawyer* 57 (January 2001).

Paul M. Schwartz, "Internet Privacy and the State: Charting a Privacy Research Agenda," 32 *Connecticut Law Review* 815 (Spring 2000).

Gregory Shaffer. "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards." 25 *Yale Journal of International Law* 1 (2000).